

WHAT IS CLAIMED IS:

1. An arithmetic operation unit for multiplying α^i when an element of $G(X) = 0$ of a primitive polynomial $G(X)$ on a Galois field) is represented by α , comprising:

a shift operating section for shifting elements by i bits before multiplication; and

a referring section for referring to a look-up table of 2^i pieces of elements when the multiplier of α is represented by i ,

wherein the element of $G(X) = 0$ of the primitive polynomial $G(X)$ on the Galois field is represented by the following expression:

$$G_{(X)} = g_m x^m + g_{m-1} x^{m-1} + g_{m-2} x^{m-2} + \dots + g_{p+1} x^{p+1} + g_p x^p + \dots + g_0.$$

2. An arithmetic operation unit for calculating $U \cdot \alpha^i$ based on an element U on a Galois field represented by the following expression:

$$U = \alpha^n u_n + \alpha^{n-1} u_{n-1} + \dots + \alpha^2 u_2 + \alpha^1 u_1 + u_0,$$

when an element of $G_{(X)} = 0$ of a primitive polynomial $G_{(X)}$ on the Galois field is represented by the following expression:

$$G_{(X)} = g_m x^m + g_{m-1} x^{m-1} + g_{m-2} x^{m-2} + \dots + g_{p+1} x^{p+1} + g_p x^p + \dots + g_0,$$

is represented by α , wherein a shift operating section for shifting the element U by i bits is ExOred with a referring section for referring to a look-up table having 2^i pieces of elements according to the least significant i bits of U.

3. An arithmetic operation unit according to claim 2, wherein when data is represented by D_1, D_2, \dots, D_k , error check symbols $E_0, E_1, E_2, \dots, E_{n-k-1}$ are calculated by the following expression:

$$D_1 + D_2 + D_3 + \dots + D_{k-1} + D_k = E_0$$

$$\alpha^k D_1 + \alpha^{k-1} D_2 + \alpha^{k-2} D_3 + \dots + \alpha^2 D_{k-1} + \alpha D_k = E_1$$

$$\alpha^{(k)^2} D_1 + \alpha^{(k-1)^2} D_2 + \alpha^{(k-2)^2} D_3 + \dots + \alpha^4 D_{k-1} + \alpha^2 D_k = E_2$$

$$\vdots$$

$$\alpha^{(k)^{n-k-1}} D_1 + \alpha^{(k-1)^{n-k-1}} D_2 + \dots + \alpha^{n-k} D_{k-1} + \alpha^{n-k-1} D_k = E_{n-k-1}$$

4. An arithmetic operation unit according to claim 3, wherein when data is decoded, symbols $S_0, S_1, S_2, \dots, S_{n-k-1}$ are obtained by calculating the following expression:

5. An arithmetic operation unit according to claim 4, wherein when the magnitude of an error is determined using the symbols $S_0, S_1, S_2, \dots, S_{n-k-1}$, the magnitude of the error is determined by providing an inverse element reference table of the form:

a) $\alpha^1, \alpha^2, \dots, \alpha^k$, and

b) $1 + \alpha^1, 1 + \alpha^2, \dots, 1 + \alpha^k$,

and by referring to the table.